Dr.WEB®
с 1992 года

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2018 года

# Обзор вирусной активности для мобильных устройств в январе 2018 года

31 января 2018 года

В январе 2018 года вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play около трех десятков игр, в которые был встроен троянец. Он незаметно скачивал и запускал вредоносные модули, способные выполнять различные действия. Кроме того, в уходящем месяце владельцам смартфонов и планшетов угрожал очередной Android-банкер, предназначенный для кражи конфиденциальной информации и денег. Также в январе в вирусную базу Dr.Web были добавлены записи для детектирования нескольких троянцев-шпионов. Среди распространявшихся вредоносных программ оказался и новый троянец-майнер, который использовал мощности зараженных мобильных устройств для добычи криптовалюты Monero.

## Главные тенденции февраля

- О бнаружение в Google Play множества игр со встроенным троянцем
- Распространение вредоносных программ, которые шпионили за владельцами мобильных устройств
- Выявление нового Android-банкера, кравшего у пользователей деньги

# Обзор вирусной активности для мобильных устройств в январе 2018 года

## Мобильная угроза месяца

В январе специалисты компании **«Доктор Веб»** обнаружили в каталоге Google Play почти **30 игр,** в которые был встроен троянец Android.RemoteCode.127.origin. Он входил в состав специализированной программной платформы для расширения функционала приложений. Android.RemoteCode.127.origin незаметно скачивал и запускал вспомогательные модули, которые могли выполнять самые разнообразные действия. Например, скрытно открывать веб-сайты и нажимать на расположенные на них рекламные ссылки и объявления, имитируя действия пользователей. Подробнее об этом троянце рассказано в нашем новостном материале.

# Обзор вирусной активности для мобильных устройств в январе 2018 года

## По данным антивирусных продуктов Dr.Web для Android


- Android.DownLoader.573.origin
  Вредоносная программа, которая загружает других троянцев, а также нежелательное ПО.

- Android.HiddenAds.171.origin
  Android.HiddenAds.253
  Android.HiddenAds.222.origin
  Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

- Android.RemoteCode.117.origin
  Троянская программа, которая скачивает и запускает различные программные модули, в том числе вредоносные.

# Обзор вирусной активности для мобильных устройств в январе 2018 года

## По данным антивирусных продуктов Dr.Web для Android


- Adware.Jiubang.2
  Adware.Jiubang.1
  Adware.Allinone.1.origin
  Adware.Adviator.6.origin

- Adware.Leadbolt.12.origin
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

# Обзор вирусной активности для мобильных устройств в январе 2018 года

## Банковский троянец

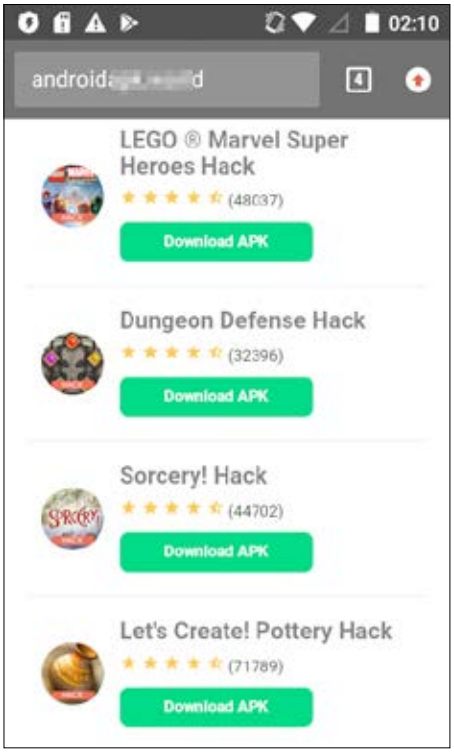
В уходящем месяце злоумышленники распространяли банковского троянца Android.BankBot.**250.origin**, который показывал поддельные окна ввода логина и пароля и передавал киберпреступникам вводимую конфиденциальную информацию. Он мог перехватывать СМС с проверочными кодами и незаметно подтверждал перевод денег на счета вирусописателей, а также другие операции в системах онлайн-банкинга.

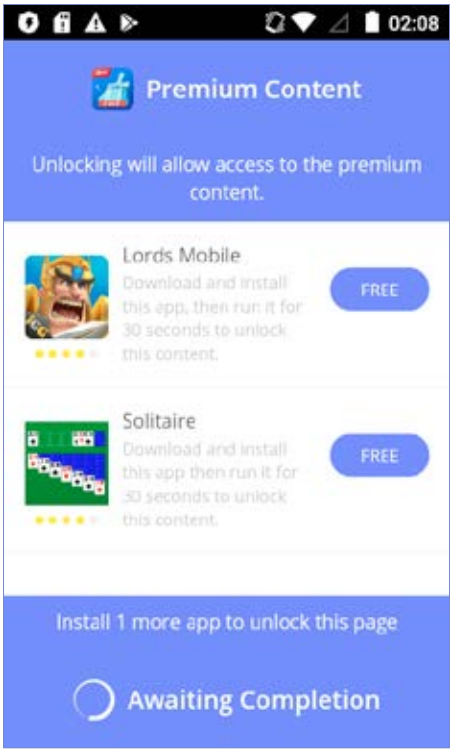
## Троянцы-шпионы

В январе в вирусную базу Dr.Web были добавлены новые записи для детектирования нескольких троянцев-шпионов. Одним из них был Android.Spy.422.**origin,** известный также под именем Dark Caracal. Злоумышленники использовали эту вредоносную программу для кибершпионажа. Android.Spy.**422.origin** похищал СМС-сообщения, отслеживал телефонные звонки, крал фотографии, историю веб-браузера и сохраненные в нем закладки, записывал окружение при помощи встроенного микрофона зараженного мобильного устройства и выполнял ряд прочих действий. Другие троянцы-шпионы представляли собой новые модификации вредоносной программы Android.Spy.**410.origin**, известной специалистам «Доктор Веб» с декабря 2017 года. Она отслеживает переписку в популярных программах, таких как Telegram, WhatsApp, Skype и других, перехватывает СМС-сообщения и телефонные звонки, а также похищает фотографии.

## Android-майнер

Среди выявленных в январе вредоносных программ для ОС Android оказался и троянец-майнер, получивший имя Android.CoinMine.8. Киберпреступники распространяли его под видом игр и программ, доступных для бесплатного скачивания на одном из веб-сайтов. В действительности все эти приложения были троянцем, который использовал зараженные устройства для майнинга криптовалюты Monero.




Злоумышленники по-прежнему создают новые вредоносные и нежелательные приложения для ОС Android и распространяют их не только через мошеннические веб-сайты, но и каталог Google Play. Для защиты мобильных устройств от таких угроз рекомендуем установить антивирусные продукты Dr.Web для Android.

# Обзор вирусной активности для мобильных устройств в январе 2018 года

## О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах